



Approved For Release 2005/04/18 : CIA-RDP82M00591R000400100013-4

NAVAL INVESTIGATIVE SERVICE

HOFFMAN BUILDING
2461 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22331

IN REPLY REFER TO

NIS-09X/bjs
5000
Ser S-0103
14 Jan 1975

SECRET (Unclassified upon removal of enclosure (2))

MEMORANDUM FOR THE WORKING GROUP ON USIB POLICY CONCERNING HAZARDOUS
ACTIVITIES RESTRICTIONS

Subj: Proposed policy

- Encl: (1) Draft of "United States Intelligence Board Security Policy
Concerning Travel and Assignment of Personnel with Access
to Sensitive Intelligence"
(2) CIA report on Risk of Capture Program

1. Forwarded for your information, review and comment is a draft of a proposed USIB policy statement to establish security guidelines applicable to the travel and assignment of personnel with access to sensitive intelligence (enclosure (1)). I plan to call a meeting of the working group during the week of 27 January 1975 to discuss this proposal if your responses indicate such is needed. Please advise me prior to that date of your views on enclosure (1).

2. Please note that the proposed policy is based on the following considerations:

a. There is no legal authority to restrict or restrain private travel directly, and attempts to do so indirectly risk legal challenge for no good purpose.

b. Experience has shown that relatively rigid restrictions so interfere with operational requirements that the restrictions are frequently waived wholesale, or, worse, waived individually on the basis of rank and influence.

c. A positive approach which recognizes both private and official needs for travel and which enlists individuals' cooperation in protecting sensitive information is far more likely to be accepted and followed than would a negative policy which attempts to restrain travel and assignments.

d. Experience has shown that preparing individuals for what they may encounter if detained or captured has been particularly useful in helping them maintain the security of sensitive information.

e. Policy in this area should extend to the protection of all sensitive intelligence, not just compartmented information.

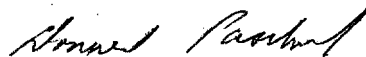
25X1

SECRET


NIS-09X/bjs
5000

f. USIB agency requirements differ, and their needs are best met by each developing and applying variations of the basic policy proposed.

3. A copy of CIA's report on their Risk of Capture Program is forwarded as enclosure (2) for your background use in connection with the review of the proposed policy. In providing that report, CIA asked that its use be limited to the members of our working group, and that it not be given general circulation in Intelligence Community agencies. Please limit the report's dissemination within your agencies accordingly.



Donald Paschal
Working Group Chairman

 Copy to: (w/encl (1) only)
Chairman, Security Committee, USIB

SECRET

UNITED STATES INTELLIGENCE BOARD SECURITY POLICY
CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL
WITH ACCESS TO SENSITIVE INTELLIGENCE

1. This establishes United States Intelligence Board security policy applicable to assignment and travel by personnel who have or have had access to sensitive intelligence (defined herein). Policy stated herein supersedes any previous intelligence community directives on this subject.
2. This policy is based on the need to protect sensitive intelligence information known to individuals from possible compromise resulting from their capture, interrogation or entrapment by hostile or unfriendly nations or groups. This policy is designed to limit the risk of compromise by providing security guidance to assist affected personnel in meeting their security responsibilities during unofficial travel and official assignments, and, in particular cases, by restricting official assignments.
3. The following definitions apply for purposes of this policy:
 - a. Sensitive intelligence consists of intelligence information, sources and methods, which involve collection techniques particularly vulnerable to hostile counteraction if compromised and which are essential to the continued provision of intelligence needed for national security. Compartmented intelligence is included in the category of sensitive intelligence, and consists of all information and materials

bearing special community controls indicating restricted handling.

Intelligence other than that which is formally compartmented should be considered sensitive for purposes of this policy only when it is subject to special controls indicating restricted handling and limited access within individual intelligence community agencies.

b. Defensive security briefings are advisories to alert persons planning travel or assignment to certain areas of risks of acts of harassment, provocation or entrapment against them by local officials. Such briefings should be based on actual experience wherever feasible, and should include information on courses of action helpful in mitigating the adverse security and personal consequences of such acts.

c. Hazardous activities include, for areas where hostilities are taking place, duties in, over or under a combat zone or behind hostile lines, and duties in isolated or exposed areas where individuals cannot reasonably be protected against hostile action. Hazardous activities also include assignment or visits to or in the immediate vicinity of, and travel through, nations which have violated, or have threatened to violate, established norms of international law and usage applicable to innocent passage or the conduct of lawful, official business.

d. Risk of capture briefings are advisories to alert persons likely to engage in hazardous activities of what they may expect in the way of attempts to force or trick them to divulge classified information if

captured or detained, and of suggested courses of action they should follow to avoid or limit such divulgence if they are captured, to include advance preparation of an innocuous, alternative explanation of their duties and background.

4. Security policies concerning travel and assignment shall provide for the following as a minimum:

a. All persons being granted or now holding access to sensitive intelligence shall be advised that they are required for the duration of access to: (1) give at least 30 days advance notice of planned travel to or through countries identified as posing a security risk; (2) obtain a defensive security briefing before traveling to such countries; (3) contact immediately the closest United States consular, attache or Embassy official if they are detained or subjected to significant harassment or provocation while traveling; and (4) report after return from travel any incidents of potential security concern which befell them. Individuals with continuing access should be reminded annually of these obligations through security education programs.

b. All persons whose access to sensitive intelligence is being or has been terminated shall be reminded of their security obligations for the continued protection of that intelligence, and shall be requested to comply with the provisions above for a stated period of time (not to exceed three years) after termination.

c. No person with access to sensitive intelligence should be officially assigned to hazardous activities without a thorough review of the nature and extent of his access balanced against operational requirements of

having that particular person's services and talents available at a designated time and place. Where the individual reviews required hereunder indicate that the risk of compromise of sensitive intelligence outweighs operational benefits, total or partial restrictions against assignment to hazardous activities should be imposed. Such restrictions should be imposed for the period of access and for brief periods thereafter (not to exceed one year). Restrictions after termination of access should be imposed only when the individuals concerned had significant knowledge of sensitive intelligence sources and methods. When individual review shows that operational requirements outweigh the risk of compromise, persons subject to this policy shall be assigned to hazardous activities only after they have been given risk of capture briefings. Hazardous activities restrictions should be applied individually by intelligence community departments and agencies to personnel assigned to, employed by, or in a contractural/consultant status with such departments and agencies.

5. USIB Principals should develop and apply security policies concerning travel and assignment consistent with the overall policy, criteria and definitions herein, and to include:

a. Developing and maintaining up to date lists of nations or areas to which such policies will apply for personnel of their departments or agencies;

b. Preparing and providing to concerned personnel of their departments or agencies security education materials on harassments or provocations against U.S. personnel traveling in or assigned to foreign nations or areas, with emphasis on acts which appear to represent attempts to compromise sensitive U.S. intelligence.

c. Preparing and providing risk of capture briefings to personnel of their departments and agencies who are being assigned duties involving hazardous activities.

Each USIB Principal should insure that his policies in these regards give due weight to the security requirements of sensitive intelligence programs managed or conducted by other USIB Principals. Each USIB Principal should also insure that new information obtained by his department or agency on harassments or provocations, and on risk of capture situations, is made available to other interested Intelligence Community member agencies, to include CIA in all cases. CIA shall maintain a central file of such information as a service of common concern.